



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/936,131	09/04/2001	Boris Balacheff	B-4295CT 619055-2	9453
22879 7590 11/01/2007 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400			EXAMINER NOBAHAR, ABDULHAKIM	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 11/01/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

MAILED

NOV 01 2007

Technology Center 2100

Application Number: 09/936,131
Filing Date: September 04, 2001
Appellant(s): BALACHEFF ET AL.

Robert Popa
Reg. No. 43,010

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed July 23, 2007 appealing from the Office action mailed December 1, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,694,536 B1	Audebert	2-2004
6,230,266 B1	Perlman et al.	5-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 2, 10-26, 28-32, 38 and 41-61 are rejected under 35 U.S.C. 102(e) as being anticipated by Audebert (6,694,436 B1).

Claims 1 and 48

Audebert discloses:

A system of computing apparatus comprising (Figs. 1-3):

a computing platform having a first data processor and a first data storage means (col. 6, lines 22-26; col. 9, lines 20-53; where the electronic unit or the server Sap corresponds to the recited computing platform);

a monitoring component having a second data processor and a second data storage means, wherein said monitoring component is configured to perform a plurality of data checks on said computing platform (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23, where the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from that application); and

a token device being physically distinct and separable from said computing platform and said monitoring component (see, for example, col. 6, lines 35-39; col. 9, lines 15-28; col. 10, lines 7-23; col. 19, lines 4-12),

wherein in one mode of operation, said token device operates to make an integrity challenge to said monitoring component and said token device will not undertake specific actions of which it is capable unless it receives a satisfactory response to said integrity challenge (see, for example, col. 2, lines 1-35; col. 4, lines 40-67; col. 21, line 59-col. 22, line 11, where the card sends the private key to the terminal only after authenticating the terminal based on a challenge/response operation).

Claims 2 and 49

Audebert discloses:

token device receives a detailed response to said integrity challenge, and processes said integrity response to interpret said integrity response (see, for example, col. 21, line 27-col. 22, line 11).

Claims 10 and 50

Audebert discloses:

token device is requested to take an action (see, for example, col. 21, lines 59-60).

Claims 11 and 51

Audebert discloses:

token device requests to take an action (col. 9, lines 54-67).

Claim 12

Audebert discloses:

The system as claimed in claim 1 in which said token device sends image data to said computer platform if a said satisfactory response to said integrity challenge is received, and said computer platform displays said image data (see, for example, col. 2, lines 34-43; col. 11, lines 30-44; col. 21, line 59-col. 22, line 11).

Claims 13 and 52

Audebert discloses:

The monitoring component is capable of establishing an identity of itself (see, for example, col. 21, line 59-col. 22, line 11, where terminal is capable to authenticate itself to the card which corresponds to the recited establishing an identity of itself).

Claims 14, 53 and 58

Audebert discloses:

The system as claimed in claim 1, further comprising an interface means for interfacing between said monitoring component and said token device (see, for example, col. 6, lines 5-15; col. 9, lines 15-25).

Claim 15 and 54

Audebert discloses:

The system as claimed in claim 1, wherein said system of computing apparatus is configured such that said monitoring component reports said data checks to said token device, said data checks containing data describing a status of said computer platform (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

Claim 16

Audebert discloses:

The system as claimed in claim 1, wherein a said specific action comprises authorizing said computing platform to undertake a transaction on behalf of a user of said system (col. 1, lines 20-37; col. 2, lines 9-67; col. 4, lines 40-67; col. 21, line 59-col. 22, line 11, where after the authentication of the terminal module by the smart card the application service provider performs the requested service by a user).

Claim 17

This claim is rejected as applied to the like elements of claim 1 as stated above and further the following:

Audebert discloses:

token device sends an integrity challenge to said monitoring component (col. 4, lines 45-55; col. 21, lines 40-67);

said monitoring component generates a response to said integrity challenge (col. 4, lines 45-55; col. 21, lines 40-67);

if said token device receives a satisfactory response to said integrity challenge, then said token device sends verification data to said computer platform, said verification data verifying correct operation of said computer platform (col. 4, lines 45-55; col. 21, lines line 59-col. 22, line 11, where the card sends the private key to the terminal only after authenticating the terminal based on a challenge/response operation and afterward the requested service by a user is provided by the application service provider i.e., by the computer platform which implies that the computer platform is authentic because it has already been authenticated by the terminal module); and

said computer platform displays said verification data on a visual display screen (see, for example, col. 2, lines 34-43; col. 11, lines 30-44; col. 21, line 59-col. 22, line 11).

Claims 18 and 59

These claims are rejected as applied to the like elements of claims 1, 13, 14 and 15 as stated above.

Claims 19 and 60

This claim is rejected as applied to the like elements of claims 1, 14 and 15 as stated above.

Claim 20

Audebert discloses:

The computing entity as claimed in claim 18, wherein said interface means is resident substantially wholly within said monitoring component (see Figs. 1; col. 9, lines 17-22).

Claim 21

Audebert discloses:

The computing entity as claimed in claim 18, wherein said interface means is comprised by said computer platform (Figs. 1; col. 9, lines 17-22, when application is on the terminal).

Claim 22

Audebert discloses:

The computing entity as claimed in claim 18, wherein said interface means comprises a PCSC stack in accordance with PCSC Workgroup PC/SC Specification 1.0 (col. 14, lines 20-67; col. 18, lines 50-67, The PC/SC Specification 1.0 is a part of ISO specifications).

Claim 23

Audebert discloses:

The computing entity as claimed in claim 18, wherein said monitoring component comprises a verification means configured to obtain a certification data independently certifying said status data, and to provide said certification data to said interface means (see, for example, col. 10, lines 7-23, where the terminal verifies the integrity of the data received from that application).

Claim 24

Audebert discloses:

The computing entity as claimed in claim 18, wherein said interface means is configured to send and receive data according to a pro-active protocol (Fig. 8a; col. 19, lines 6-40).

Claim 25

Audebert discloses:

A method of obtaining verification of a state of a computer entity (Fig. 9), said computer entity comprising a computer platform comprising a first data processor and a first memory means (Fig. 3; col. 6, lines 22-26; col. 9, lines 20-53; where the electronic unit or the server Sap corresponds to the recited computing platform), and a monitoring component comprising a second data processor and a second memory means (see, for example, abstract; col. 6, lines 26-33, where the terminal corresponds to the recited monitoring component), said method comprising the steps of:

receiving an interrogation request signal via an interface of said computing entity (see, for example, col. 6, lines 22-34;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23, where the terminal authenticates the application on the electronic unit or server and verifies the integrity of the data received from that application); and

said monitoring component reporting a result message to said interface said result message describing a result of said monitoring operation (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

Claim 26

Audebert discloses:

A method as claimed in claim 25, in which said monitoring operation comprises the steps of:

said monitoring component carrying out one or a plurality of data checks on components of said computing platform (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23); and

said monitoring component being able to report a set of certified reference data together with said data check (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

Claim 28

This claim is rejected as applied to the like elements of claim 15 as stated above.

Claim 29

Audebert discloses:

The method as claimed in claim 25, wherein said result message is transmitted by said interface to a token device external of said computing entity (see, for example, Fig. 1 and Fig. 3).

Claim 30

Audebert discloses:

The method as claimed in claim 25, comprising the step of reporting a result of said monitoring operation by generating a visual display of confirmation data (see, for example, col. 2, lines 34-43; col. 11, lines 30-44; col. 21, line 59-col. 22, line 11).

Claim 31

Audebert discloses:

The method as claimed in claim 25, further comprising the step of adding a digital signature data to said result message, said digital signature data identifying said monitoring component; and transmitting said result message and said digital signature data from said interface (col. 2, line 25-45; col. 10, lines 50-65; col. 11, lines 56-65).

Claim 32

Audebert discloses:

A method of obtaining verification of a state of a computer entity, said computer entity comprising a computer platform and a monitoring component, said method comprising the steps of:

an application requesting access to a functionality from a token device (see, for example, col. 1, lines 20-37; col. 1, line 63-col. 2, line 32; col. 3, lines 42-50);

in response to said request for access to functionality said token device generating a request signal requesting a verification data from said monitoring component (see, for example, col. 1, line 63-col. 2, line 32);

in response to said request for verification, said monitoring component reporting a result message to said token device, said result message describing a result of a monitoring operation (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

by receipt of a satisfactory said result message, said token device offers said functionality to said application (col. 2, lines 15-27; col. 4, lines 40-60).

Claim 38

Audebert discloses:

A method of checking an integrity of operation of a computing entity, said computing entity comprising a computer platform having a first processor means and first data storage means (Fig. 3; col. 6, lines 22-26; col. 9, lines 20-53; where the electronic unit or the server Sap corresponds to the recited computing platform), and a monitoring component comprising a second data processor and a second memory means (see, for example, abstract; col. 6, lines 26-33, where the terminal corresponds to the recited monitoring component), by means of a token device, said token device

Art Unit: 2132

comprising a third data processor and a third memory means (col. 2, lines 4-15), said method comprising the steps of:

programming said token device to respond to a received poll signal from an application program, said poll signal received from said computer platform; said token device receiving a poll signal from said computer platform (see, for example, col. 1, lines 20-37; col. 1, line 63-col. 2, line 32; col. 3, lines 42-50);

in response to said received poll signal, said token device generating a signal for requesting a verification operation by said monitoring component (see, for example, col. 1, line 63-col. 2, line 32); and

said monitoring component performing a verification operation of said computer platform in response to said received signal from said token device (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23, where the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from that application).

Claim 42

Audebert discloses:

A method of verifying a status of a computing entity, by means of a token device provided external of said computing entity said method comprising the steps of:

said token device receiving a poll signal (see, for example, col. 1, lines 20-37; col. 1, line 63-col. 2, line 32; col. 3, lines 42-50);

said token device responding to said poll signal by providing a request for obtaining verification of a state of said computer entity (see, for example, col. 1, line 63-col. 2, line 32); and

said token device receiving a result message, said result message describing the result of said verification (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

Claim 43

Audebert discloses:

A method by which a token device can obtain verification of a state of a computing platform by using a monitoring component (col. 2, lines 4-15),

said monitoring component being capable of performing at least one data check on said computer platform (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23, where the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from that application), and establishing an identity of itself (see, for example, col. 21, line 59-col. 22, line 11, where terminal is capable to authenticate itself to the card which corresponds to the recited establishing an identity of itself), and establishing a report of said at least one data check (see, for example, col. 10, lines 4-22, wherein the terminal first verifies i.e., authenticates the

Art Unit: 2132

application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device); and

wherein said token device has data processing capability and behaves in an expected manner (col. 2, lines 4-15);

said token device being physically separable from said computing platform and said monitoring component (Figs. 1 and 3), said token device having cryptographic data processing capability (col. 2, lines 5-35)

wherein, said monitoring component proves its identity to said token device and establishes a report to said token device of at least one data check performed on said computer platform (see, for example, col. 4, lines 40-67; col. 10, lines 4-22; col. 21, line 59-col. 22, line 11; wherein the terminal first verifies i.e., authenticates the application installed on the server and then sends commands to the card which indicates to the card that the server is secured and authentic and corresponds to the recited reports said data checks to said token device).

Claim 44

Audebert discloses:

A token device comprising a data processor and a memory device, said token device configured to perform at least one data processing or signaling function (col. 2, lines 4-15):

wherein said token device operates to:

receive an integrity check data from an external source see, for example, col. 1, lines 20-37; col. 1, line 63-col. 2, line 32);

if said integrity check data supplied to said token device is satisfactory, then said token device allows a said function (see, for example, col. 2, lines 1-35; col. 4, lines 40-67; col. 21, line 59-col. 22, line 11, where the card sends the private key to the terminal only after authenticating the terminal based on a challenge/response operation); and

if said integrity check data received by said token device is unsatisfactory, then said token device denies said function (see, for example, col. 1, lines 50-66; col. 12, lines 5-26; col. 23, lines 43-55).

Claim 41

This claim is rejected as applied to the like elements of claims 22, 24 and 32 as stated above.

Claims 45-47 and 57

Audebert discloses:

A system as claimed in claims 1, 18, 44 and 48, wherein said token device is a smart card (col. 10, lines 7-14).

Claim 55

Audebert discloses:

The system as claimed in claim 48, wherein the monitoring component is mounted on a common assembly with the first processor (see, for example, col. 1, lines 37-45; col. 10, lines 37-43).

Claim 56

Audebert discloses:

The system as claimed in claim 48, wherein one or more of said data checks comprise a check of the integrity of the basic input/output software for one or more components of the computing apparatus (see, for example, abstract; col. 6, lines 26-33; col. 7, lines 3-18; col. 10, lines 7-23, where the terminal corresponds to the recited monitoring component which authenticates the application on the electronic unit or server and verifies the integrity of the data received from that application).

Claims 58 and 61

Audebert discloses:

The system as claimed in claim 53, wherein the portable user token is a smart card, and the token interface comprises a smart card reader (col. 2, lines; col. 2, lines 57-63; 3-8; col. 10, lines 7-14).

Claims 3-9 and 33-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Audebert (6,694,436 B1) in view of Perlman et al (6,230,266 B1, hereinafter Perlman).

Claims 3-5, 9, 33 and 34

Audebert does not expressly disclose that the system as claimed in claim 1, further comprising a third party server, wherein a response to said integrity challenge is sent to said third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Audebert by the teaching of Perlman, because it would provide a technique to ascertain if a computing element has been compromised (Perlman, col. 4, lines 22-28).

Claims 6, 7, 35 and 36

Audebert discloses:

a server sends a simplified integrity response to said token device (see, for example, col. 1, lines 20-37; col. 1, line 63-col. 2, line 32; col. 3, lines 42-50).

Audebert does not expressly disclose that the system as claimed in claim 32, comprises a third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Audebert by the teaching of Perlman, because it would provide a technique to ascertain if a computing element has been compromised (Perlman, col. 4, lines 22-28).

Claims 8 and 37

Audebert discloses:

The method as claimed in claim 32, further comprising the steps of:

adding a digital signature data to a simplified integrity response, said digital signature data authenticating a server to said token device (col. 2, line 25-45; col. 10, lines 50-65; col. 11, lines 56-65).

Audebert does not expressly disclose that the system as claimed in claim 32, comprises a third party server.

Perlman teaches a system having a server that receives information from a verifying principal (corresponding to the recited token device or monitoring component) to verify the status of a certificate (col., line 56-col. 6, line 1-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Audebert by the teaching of Perlman,

because it would provide a technique to ascertain if a computing element has been compromised (Perlman, col. 4, lines 22-28).

Allowable Subject Matter

Claim 27 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

(10) Response to Argument

10.1 Appellants, on page 8 through page 9 of the Appeal Brief, argue that: "the terminal of Audebert does indeed verify the integrity of data received from the server, this is not the same as performing data checks on the server. The terminal of Audebert first receives data from the server and then, once the received data is in its possession, verifies its integrity - in other words, the terminal performs data integrity checks on the terminal, not on the server."... "Audebert teaches no more than verifying the identity of the server as it is coded into the transmitted data, and does not undertake any actions that can be understood as verifying the integrity of the server."... "verifying the *origin* of data is not the same as verifying the *integrity of the origin* of data."

Examiner respectfully disagrees because the claims 1, 17, 18, 26, 43, 48 and 59 of the instant application recite that the monitoring component performs data check(s) on the computing platform and claim 38 of the instant application recite that the monitoring component performs a verification operation of the computing platform.

These claims do not recite or specify how the data check and the verification operation are being performed. Claim 19 recites that the monitoring component for the purpose of performing a monitoring operation on the computer platform obtains (i.e., receives) data describing an operating status of the computer platform and claim 23 recites that the monitoring component comprises a verification means that obtains a certification data to certify the status data of the computer platform. Thus, according to claims 19 and 23, the monitoring component receives some information related to the computer platform in order to perform either data check or verification operation on the computer platform, which is the same what being taught in Audebert. Audebert teaches a system comprising a terminal module (corresponding to the recited monitoring component) that receives information from a server (corresponding to the recited computer platform) (col. 6, lines 26-28, col. 9, lines 13-19 and lines 58-63 and col. 10, lines 40-49) in order to identifying and/or authenticating the source of requests sent by the application (Fap) installed in the electronic unit (corresponding to the recited computer platform) (abstract, lines 16-17 and col. 7, lines 5-8). Furthermore, Audebert teaches that the filter installed on the terminal module checks the origin and integrity of the request sent by the server (i.e., computer platform) (col. 9, lines 58-59, col. 10, lines 10-15, col. 10, lines 55-59 and col. 28, lines 20-29).

10.2 With regard to claim 25, appellants, on page 9 of the Appeal Brief, argue that: "Appellants have previously explained that there is in fact no interrogation request signal received by the server (computing platform) of Audebert; on the contrary, the

requests in Audebert flow from the server to the terminal. There are no requests flowing from the terminal to the server because the terminal verifies the identity of the server solely based on the information contained in the requests received from the server.'

Examiner respectfully disagrees because the claim 25 of the instant application recites:

"receiving an interrogation request signal via an interface of said computing entity;

said monitoring component performing a monitoring operation of said computer platform in response to a said received interrogation request signal", which is contrary to the appellant argument, because it is evident from the claim language that the request is received by monitoring component from the computer platform. Audebert teaches that the application installed on the electronic unit (i.e., the server) sends a request to the terminal unit related to a user transaction process (corresponding to the recited receiving an interrogation request) and then the terminal unit authenticates the origin of the request (i.e., the server) (corresponding to the recited performing a monitoring operation) (see, for example, col. 6, lines 22-43, col. 7, lines 5-8, col. 9, lines 54-62 and col. 10, lines 7-14).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Abdulahkim Nobahar *A.N.*

Examiner, Art Unit 2132

Gilberto Barron Jr.
GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

October 26, 2007

Conferees:

Gilberto Barron *GB*

Matthew Smithers

/Matthew Smithers/
Primary Examiner
AU 2137